SHARING ACCOUNT DATA BETWEEN DIFFERENT INTERFACES TO A SERVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a divisional application of U.S. patent application Ser. No. 14/289,619, entitled "Sharing Account Data Between Different Interfaces to a Service," filed on May 28, 2014, which is hereby incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Many mobile devices (e.g., smart phones, tablets) use native applications, or apps, to access various web-based services. For example, various social media, photo-sharing, streaming video, and other web-based services develop their own applications for mobile device operating systems. FIG. **1** illustrates an example of such a web-based service entity **100**, to which both a mobile device **105** and a laptop computer **110** connect through the Internet **115** (while laptops are, of course, mobile, this document uses mobile device to primarily refer to devices such as smart phones and tablets that run on mobile operating systems).

[0003] As shown in FIG. **1**, in some cases these devices may connect to different servers provided by the web-based service entity **100** (the mobile device **105** connecting through a native application to the mobile app server **120** and the laptop computer connecting through a web browser to the web server **125**). The web-based entity stores passwords and other user data for the users of these devices, which is used by both the web server and the mobile app server. However, the user has to login to the entity separately on the mobile device **105** and the laptop **110**, as well as for any other devices. In addition, the user may access the web server via a web browser on the mobile device, and would have to log in separately from the application login. This requires the user to remember and enter all of their passwords each time they acquire a new device.

BRIEF SUMMARY

[0004] Some embodiments provide a framework to enable one or more devices to share user data related to a third party entity (e.g., a web-based content or service provider). The framework enables different interfaces that access the same third party entity to use the shared data, and pass the shared data between each other. For example, in some embodiments, a web browser that accesses the third party entity via a website and an application provided by the third party entity for accessing the entity share data with each other via a data repository on the device or devices on which they operate.

[0005] When a first one of the interfaces wants to use data stored on the device by a second interface, in some embodiments the first interface provides a request to the device (e.g., to the operating system of the device, or to a background application operating on the device) to enable sharing of data between itself and the second interface. The device determines whether the first and second interfaces are verified to share data with each other (e.g., by checking a database of verified trust relationships). If the two interfaces are verified, the device releases the requested account data to the requesting interface.

[0006] In some embodiments, in order to determine whether two interfaces may share user data, the device stores a database of verified interface partnerships and types of data. For instance, the database of some embodiments stores a set of application-web domain pairings, for applications that access the same third party as a web browser connecting to the web domain. Each pairing, in some embodiments, further specifies a type of account data that may be shared between the two interfaces (e.g., credentials such as a username, password, username/password combination, tokens such as OAuth tokens, HTTP cookies, etc., task continuation data specifying the user's most recent interactions with a third party entity, or other data associated with a user account or the user's interactions with the third party entity).

[0007] As mentioned, in order for two interfaces on a device (or on separate devices) to share user data with each other, some embodiments require that a relationship between the interfaces be verified by one of the devices. For instance, in the case of a web domain and application using the same account data, in some embodiments (i) the application provides data identifying the web domain for data sharing, and (ii) the web domain separately provides data identifying the application for data sharing. Similarly, two web domains or two applications can provide data identifying each other for user data sharing. In some embodiments, the two interfaces also specify the type of user data to be shared (e.g., credentials, task continuation data, etc.).

[0008] In some embodiments, the application provides its own application identifier and a set of web domains (e.g., www.xyz.com) and shared account data types (e.g., password). The device then contacts the web server at the specified domain in order to receive a certified list of associated applications for user data sharing and the types of data to be shared (e.g., signed with a certificate issued from a trusted certification authority). When the requesting application is on the list received from the web server, the device stores the verified relationship in a database in order to provide the verified account data to the application.

[0009] Similarly, two applications might share data by providing each other's application identifiers to the device for verification, rather than providing a web domain. Two web domains (e.g., www.xyz.com and mobile.xyz.com) could list each other for account data sharing as well.

[0010] The preceding Summary is intended to serve as a brief introduction to some embodiments of the invention. It is not meant to be an introduction or overview of all inventive subject matter disclosed in this document. The Detailed Description that follows and the Drawings that are referred to in the Detailed Description further describe the embodiments described in the Summary as well as other embodiments. Accordingly, to understand all the embodiments described by this document, a full review of the Summary, the Detailed Description, and the Drawings is needed. Moreover, the claimed subject matters are not to be limited by the illustrative details in the Summary, the Detailed Description, and the Drawings, but rather are to be defined by the appended claims, because the claimed subject matters can be embodied in other specific forms without departing from the spirit of the subject matters.